REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Personal Interview

Applicant wishes to also thank the Examiner for taking the time to meet with the undersigned, John R.S. Orange (29,725), and Dr. Scott Vanstone in a personal interview on October 18, 2007. In the personal interview, proposed claim amendments were discussed to clarify the distinctions over the references previously cited against the current claims. It was agreed that the references cited do not recognize the bias that may be introduced by the selection of k. To clarify this distinction, amendments to claims 1 and 9 were proposed that specify that the step of determining whether or not the output is less than the order q is done prior to reducing mod q. The Schneier reference does not teach accepting or rejecting a key by checking that it is less than q before reducing mod q. As explained by Dr. Vanstone, and discussed in the background of the present application, the Schneier reference, which refers to DSA and the DSS, requires the reduction of the integer mod q which can expect that more values will lie in the first interval than the second, hence the bias. It has been recognized by Applicant that by first checking that the output to be used as the key is less than q and then accepting or rejecting based on this determination can avoid the bias altogether. Again, the proposed amendments are believed to clarify this distinction. It was agreed in the personal interview that neither the Vanstone reference, nor the Schneier paper recognize the bias let alone teach the making such a determination prior to reducing mod q. As such, it is believed that the amendments outlined above clearly and patentably distinguish over the references cited in the final rejection.

Status of Application

Applicant advises that a Notice of Appeal was filed on July 17, 2007 along with a request for a one-month extension of time. The present response is being filed concurrently with a request for continued examination (RCE) and a request for a two-month extension of time to reopen prosecution. It is believed that the present application should now be taken out of the appeal process and that in view of the present response, the RCE is proper. As such, the above-noted amendments should be entered and prosecution be continued on the basis of such amendments.

Claim Amendments

As discussed above, claims 1 and 9 have been amended to clarify that the step of determining if the output is less than the order q is done "prior to reducing mod q". New claims

15-22 have been added, which are directed to a computer readable medium with instructions for performing the steps which are believed to be allowable in claims 1-14. New claims 23-30 have been added, which are similar to claims 15-22 but are directed to a cryptographic unit.

No new subject matter is believed to have been added by way of these amendments.

Claim Rejections

Claims 1, 2, 4 and 5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone (US 6,195,433) in view of Schneier (Applied Cryptography). As discussed above, claim 1 has been amended to specify that the step of determining whether or not the output is less than the order q is done prior to reducing mod q. The Schneier reference does not teach accepting or rejecting a key by checking that it is less than q before reducing mod q. As explained by Dr. Vanstone in the personal interview, and discussed in the background of the present application, the Schneier reference, which refers to DSA and the DSS, requires the reduction of the integer mod q which can expect that more values will lie in the first interval than the second, hence the bias. It has been recognized by Applicant that by first checking that the output to be used as the key is less than q and then accepting or rejecting based on this determination can avoid the bias altogether. As such, claim 1, as amended, is believed to clearly and patentably distinguish over the cited references. Claims 2, 4 and 5 being ultimately dependent on claim 1 are also believed to be distinguished.

Claims 7-13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, in view of Schneier, in further view of Matyas, in further view of Backal. It is believed to have been shown above that claims 1 and 9 clearly and patentably distinguish over Vanstone in view of Schneier. As previously argued, neither Matyas nor Backal have recognized the bias discussed above, let alone teach accepting or rejecting an output to be used as a key prior to reducing mod q. As such, neither Matyas nor Backal teach what is missing from Vanstone and Scheier. Claims 7-13, are therefore also believed to be patentably distinguished over the cited references.

Claims 3, 6 and 14 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, in view of Schneier, in further view of Matyas (alone or in combination with Backal). Claims 3, 6 and 14 being ultimately dependent on either claim 1 or claim 9 are believed to be distinguished for reasons similar to those expressed above.

Claims 1, 2, 4 and 5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier view of Matyas, in further view of Patel (US 6,327,660). Again, as previously argued, Patel does not teach what is believed to have been shown to be missing from Schneier

Claims 7-13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier view of Matyas, in further view of Patel, in further view of Backal. Similar arguments equally apply to this rejection as this is simply another combination of references that fails to teach the bias recognized by Applicant and the features recited in claims 1 and 9.

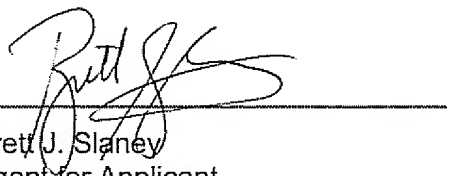
Claims 3, 6 and 14 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier view of Matyas, in further view of Patel (alone or in combination with Backal). Similar arguments equally apply to this rejection as this is simply another combination of references that fails to teach the bias recognized by Applicant and the features recited in claims 1 and 9.

Summary

In view of the foregoing, it is believed that claims 1, 9, as amended, and those claims dependent thereon, are clearly and patentably distinguished over the references cited by the Examiner and thus are in condition for allowance. New claims 15-30 are also believed to be patentably distinguished for similar reasons.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



Brett J. Slaney
Agent for Applicant
Registration No. 58,772

Date: October 30, 2007

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416-863-2518
BS/